UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

David Pawlik, on Behalf of Himself and all Others Similarly Situated, Plaintiff, v. Yahoo!, Incorporated, Defendant.	Case No. 16-cv-9011 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff David Pawlik ("Plaintiff"), on behalf of himself and all other New York residents similarly situated, files this Class Action Complaint ("Complaint") against Defendant Yahoo!, Incorporated ("Yahoo" or "Defendant"), and respectfully alleges the following:

NATURE OF THE ACTION

1. This class action seeks to redress Yahoo's unlawful and negligent disclosure of millions of users' accounts, which included users' confidential personal information, in violation of New York General Business Law § 349 and common law.

2. Defendant failed to fulfill its legal duty to protect Yahoo users' personal identifying information ("PII") which was stored in its systems. Yahoo recklessly and negligently disregarded is obligations to safeguard users' PII which resulted in a massive data breach in late 2014 ("Data Breach" or "Breach").

JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction over Plaintiff's claims pursuant to 28 U.S.C. § 1332(d) (CAFA) because (a) there are 100 or more Class Members, (b) at least one Class Member is a citizen of a state that is diverse from Yahoo's citizenship, and (c) the matter in controversy exceeds $5 million, exclusive of interest and costs.

4. This Court has personal jurisdiction over Yahoo! Because Yahoo! Is registered to

conduct business in New York and has sufficient minimum contacts with New York.

5. Venue is appropriate in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in in this District.

PARTIES

6. Plaintiff David Pawlik is a resident of New York County, New York. Plaintiff has held a Yahoo user account for more than a decade which he regularly uses for personal email correspondence. Plaintiff provided confidential information to Defendant including his name, email address, and date of birth in connection with his Yahoo account registration. Additionally, Plaintiff created a unique password to access his account. Plaintiff uses his Yahoo user account for a variety of personal purposes and reasonably expected that Defendant would maintain the privacy of his confidential account information. Given the broad scope of the Data Breach, Plaintiff's account was almost certainly amongst those included in the Data Breach. After learning of the breach, Plaintiff has spent numerous hours monitoring his accounts and addressing issues arising from the Data Breach, and purchased credit monitoring services to mitigate any damage in connection with the Data Breach.

7. Defendant Yahoo!, Incorporated is incorporated in the state of Delaware with its principal place of business in Sunnyvale, California.

FACTS

I. Yahoo's Data Breach

8. Yahoo is a large technology company that provides various services including personal email accounts. According to Defendant Yahoo's press release regarding this data breach:

> Yahoo is a guide to digital information discovery, focused on informing, connecting, and entertaining through its search, communications, and digital content products. By creating highly personalized experiences, Yahoo helps users discover the information that matters most to them around the world -- on mobile or desktop. Yahoo connects advertisers with target

> audiences through a streamlined advertising technology stack that combines the power of Yahoo's data, content, and technology.[1]

9. Yahoo collects and stores account holders' PII in connection with their user accounts. This data includes, but is not limited to, first and last names, birthdays, telephone numbers, email addresses, and unique account passwords.

10. PII is of great value and Yahoo has a duty to take every reasonable measure to protect user information and safeguard it from unlawful disclosures or theft.

11. Yahoo represents in its Privacy Policy that it will safeguard users' PII. When Plaintiff and members of the Class signed up for Yahoo accounts, they entrusted Yahoo with their PII with the understanding that Yahoo would safeguard that information. That expectation was reinforced by Yahoo's Privacy Policy, which provides that Yahoo has "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you."[2]

12. Defendant Yahoo is and, at all times relevant, was keenly aware of the risks associated with compiling massive amounts of its users' PII and that protecting its users' PII was very important to its business. In fact, Defendant Yahoo made the following representations about its data security practices in its 2015 Annual Report:[3]

> ***Changes in regulations or user concerns regarding privacy and protection of user data, or any failure to comply with such laws, could adversely affect our business.***
>
> Federal, state, and international laws and regulations govern the collection, use, retention, disclosure, sharing and security of data that we receive from and about our users. The use of consumer data by online service providers and advertising networks is a topic of active

[1] *See* "An Important Message to Yahoo Users on Security," (Nov. 16, 2016), https://investor.yahoo.net/releasedetail.cfm?ReleaseID=990570 (last visited Nov. 16, 2016).

[2] *See* YAHOO!: PRIVACY POLICY, https://policies.yahoo.com/sg/en/yahoo/privacy/index.htm (last visited Nov. 16, 2016).

[3] *See* Yahoo!, Inc.'s 2015 Annual Report, http://files.shareholder.com/downloads/YHOO/2908978308x0x893458/96E76DB6-C10F-4514-AAB0-24BFC488B422/yahoo_ar15_annual_report.pdf (last visited Nov. 16, 2016).

interest among federal, state, and international regulatory bodies, and the regulatory environment is unsettled. Many states have passed laws requiring notification to users where there is a security breach for personal data, such as California's Information Practices Act. We face similar risks in international markets where our products, services and apps are offered. **Any failure, or perceived failure, by us to comply with or make effective modifications to our policies, or to comply with any federal, state, or international privacy, data-retention or data-protection-related laws, regulations, orders or industry self-regulatory principles could result in proceedings or actions against us by governmental entities or others, a loss of user confidence, damage to the Yahoo brands, and a loss of users, advertising partners, or Affiliates, any of which could potentially have an adverse effect on our business.**

In addition, various federal, state and foreign legislative or regulatory bodies may enact new or additional laws and regulations concerning privacy, data retention, data transfer and data protection issues, including laws or regulations mandating disclosure to domestic or international law enforcement bodies, which could adversely impact our business, our brand or our reputation with users.

…

If our security measures are breached, our products and services may be perceived as not being secure, users and customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure.

Our products and services involve the storage and transmission of Yahoo's users' and customers' personal and proprietary information in our facilities and on our equipment, networks and corporate systems. Security breaches expose us to a risk of loss of this information, litigation, remediation costs, increased costs for security measures, loss of revenue, damage to our reputation, and potential liability. Outside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information to gain access to our data or our users' or customers' data. In addition, hardware, software or applications we procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise network and data security.

Additionally, some third parties, such as our distribution partners, service providers and vendors, and app developers, may receive or store information provided by us or by our users through applications integrated with Yahoo. If these third parties fail to adopt or adhere to

> adequate data security practices, or in the event of a breach of their networks, our data or our users' data may be improperly accessed, used or disclosed. Security breaches or unauthorized access have resulted in and may in the future result in a combination of significant legal and financial exposure, increased remediation and other costs, damage to our reputation and a loss of confidence in the security of our products, services and networks that could have an adverse effect on our business. We take steps to prevent unauthorized access to our corporate systems, however, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently or may be designed to remain dormant until a triggering event, we may be unable to anticipate these techniques or implement adequate preventative measures. If an actual or perceived breach of our security occurs, the market perception of the effectiveness of our security measures could be harmed and we could lose users and customers.

13. Defendant Yahoo represents in its Privacy Policy that it will safeguard users' PII:[4]

> **Confidentiality & Security**
>
> We limit access to personal information about you to employees who we believe reasonably need to come into contact with that information to provide products or services to you or in order to do their jobs.
>
> We have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you.

14. Defendant Yahoo further represents the type of security it promised to Plaintiff and Class members on its website:[5]

> **Security at Yahoo**
>
> Protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users' trust. We have taken the following measures to protect your information:
>
> **Transport Layer Security (TLS)**

[4] *See* YAHOO!: PRIVACY POLICY, https://policies.yahoo.com/sg/en/yahoo/privacy/index.htm (last visited Nov. 16, 2016).

[5] *See* SECURITY AT YAHOO, https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm (last visited Nov. 16, 2016).

> We use TLS encryption when transmitting certain kinds of information, such as financial services information or payment information. An icon resembling a padlock is displayed in most browsers during TLS sessions.
>
> **Second Sign-in Verification**
>
> You may turn on a setting that requires a second piece of information such as a code sent via SMS - in addition to your password - when signing in to your account from a device or location we don't recognize. Learn more about second sign-in verification.
>
> **On-Demand Passwords**
>
> Yahoo also offers on-demand passwords. By linking your mobile device to your account, you enable Yahoo to provide you with an on-demand password sent to your mobile phone, so you don't have to remember passwords anymore. Learn more about on-demand passwords.
>
> **Secure Storage**
>
> We deploy industry standard physical, technical, and procedural safeguards that comply with relevant regulations to protect your personal information.

15. When Plaintiff and Class members signed up for Yahoo accounts, they entrusted Defendant Yahoo with their PII with the understanding that Defendant Yahoo would safeguard that information. That expectation was reinforced and by Yahoo's Privacy Policy and other statements about security.

16. In a September 22, 2016 statement, Yahoo confirmed that certain user data for approximately 500 million users was stolen from Defendant in late 2014.[6]

17. Yahoo confirmed that the compromised data may have included "names, email addresses, telephone numbers, dates of birth, hashed passwords . . . and in some cases, encrypted

[6] *See* Seth Fiegerman, *Yahoo Says 500 Million Accounts Stolen,* CNN MONEY (Sept. 22, 2016, 11:30 PM), http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/.

or unencrypted security questions and answers."[7] Such security questions frequently include place of birth and mother's maiden name.

18. On September 27, 2016, Senators Patrick Leahy, Al Franken, Elizabeth Warren, Richard Blumenthal, Ron Wyden and Edward Markey wrote to Marissa Mayer, Yahoo's Chief Executive Officer, demanding that Yahoo explain why the Data Breach was only recently announced despite the fact that the data was stolen approximately two years prior:

> We are even more disturbed that user information was first compromised in 2014, yet the company only announced the breach last week. That means millions of American's data may have been compromised for two years. This is unacceptable. This breach is the latest in a series of data breaches that have impacted the privacy of millions of American consumers in recent years, but it is by far the largest. Consumers put their trust in companies when they share personal and sensitive information with them, and they expect all possible steps be taken to protect that information.
>
> In light of these troubling revelations, please answer the following questions to help Congress and the public better understand what went wrong and how Yahoo intends to safeguard data and protect its users, both now and in the future. We also request that Yahoo provide a briefing to
> our staff on the company's investigation into the breach, its interaction with appropriate law enforcement and national security authorities, and how it intends to protect affected users.
>
> 1. When and how did Yahoo first learn that its users' information may have been compromised? Please provide a timeline detailing the nature of the breach, when and how it was discovered, when Yahoo notified law enforcement or other government authorities about the breach, and when Yahoo notified its customers.
>
> 2. Press reports indicate the breach first occurred in 2014, but was not discovered until August of this year. If this is accurate, how could such a large intrusion of Yahoo's systems have gone

[7] Bob Lord, *An Important Message About Yahoo User Security Yahoo*, YAHOO! (Sept. 22, 2016), https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security (last visited Sep. 23, 2016).

undetected?

3. What Yahoo accounts, services, or sister sites have been affected?

4. How many total users are affected? How were these users notified?

5. What protection is Yahoo providing the 500 million Yahoo customers whose identities and personal information are now compromised?

6. What steps can consumers take to best protect the information that may have been compromised in the Yahoo breach?

7. What is Yahoo doing to prevent another breach in the future? Has Yahoo changed its security protocols, and in what manner?

8. Did anyone in the U.S. government warn Yahoo of a possible hacking attempt by state sponsored hackers or other bad actors? When was this warning issued?[8]

19. At this time, it is unclear when Yahoo learned of this massive breach, why it took two years to discover the breach, or if Yahoo delayed informing its customer that it failed to monitor their PII. Such a delay is damaging to Yahoo users in that they could have immediately acted in a manner to protect themselves and their PII from further harm.

20. Some experts are calling this disclosure "the biggest data breach ever."[9]

II. Personally Identifiable Information (PII)

21. PII is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners.

22. PII is information that can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and biometric records. This can be

[8] Letter from Senators Patrick Leahy, Al Franken, Elizabeth Warren, Richard Blumenthal, Ron Wyden and Edward Markey, Sept. 27, 2016 at https://www.leahy.senate.gov/imo/media/doc/9-27-16%20Yahoo%20Breach%20Letter.pdf (last accessed Nov. 16, 2016).

[9] *See* Dustin Volz, *Hackers Steal Data From 500 Million Yahoo Accounts*, REUTERS (Sept.t 22, 2016) http://uk.reuters.com/article/us-yahoo-cyber-idUKKCN11S16P?il=0.

accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[10]

23. PII does not include only data that can be used to directly identify or contact an individual (*e.g.*, name, e-mail address), or personal data that is especially sensitive (*e.g.*, Social Security number, bank account number, payment card numbers).[11]

24. Given the nature of this breach, it is foreseeable that the compromised PII can be used to access Plaintiff and the Class Members' user accounts, providing access to additional PII or personal and sensitive information.

25. Therefore, the compromised PII in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways.

26. Indeed, in August 2016, it was first rumored that a hacker gained access to Yahoo's data systems and was selling data for approximately 200 million Yahoo users.[12]

27. At that time, Yahoo was aware of the claim, but did not confirm the legitimacy of the rumors.[13]

28. For example, "[t]hese harms may include the unexpected revelation of previously private information, including both sensitive information (*e.g.*, health information, precise

[10] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

[11] *See, e.g.*, NAT'L INST. OF STANDARDS & TECHNOLOGY, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII), NIST SPECIAL PUBLICATION 800-122 (April 2010), at E.S.-1, 2-1.

[12] *See* Kara Swisher, *Yahoo Is Expected To Confirm A Massive Data Breach, Impacting Hundreds Of Millions Of Users*, RECODE (Sept. 22, 2016, 2:18 AM), http://www.recode.net/2016/9/22/13012836/yahoo-is-expected-to-confirm-massive-data-breach-impacting-hundreds-of-millions-of-users.

[13] *See Id.*

geolocation information) and less sensitive information (*e.g.*, purchase history, employment history) to unauthorized third parties."[14]

29. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves.

30. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[15]

31. For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[16]

32. Further, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."[17]

33. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts particularly when they have easily-decrypted passwords and security questions. Bcrypt encryption is easily cracked by hackers and identity thieves.

34. Unfortunately for Plaintiff and Class Members, a person whose PII has been

---

[14] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (March 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[15] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, PRELIMINARY FTC STAFF REPORT 35-38 (Dec. 2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[16] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device")

[17] FEDERAL CHIEF INFORMATION OFFICERS COUNCIL, RECOMMENDATIONS FOR STANDARDIZED IMPLEMENTATION OF DIGITAL PRIVACY CONTROLS (Dec. 2012), at 7-8.

compromised may not fully experience the effects of the breach for years to come:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[18]

35. Accordingly, Plaintiff and the Class Members will bear a heightened risk for years to come.

36. Identity theft is one such risk and occurs when an individual's PII is used without his or her permission to commit fraud or other crimes.[19]

37. According to the Federal Trade Commission, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[20]

38. As a direct and proximate result of Yahoo's reckless and negligent actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class Members' PII, Plaintiff and the Class are susceptible to imminent and certainly impending injury flowing from identity theft.

39. As a result of Yahoo's actions compromising their personal information, Plaintiff and Class members will face an increased risk of experiencing the following injuries:

---

[18] G.A.O., PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (June 2007), http://www.gao.gov/assets/270/262904.html.

[19] *See* FEDERAL TRADE COMMISSION: TAKING CHARGE: WHAT TO DO IF YOUR IDENTITY IS STOLEN (April 2013), https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

[20] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (March 2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

- money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;
- money and time lost as a result of fraudulent access to and use of their financial accounts;
- loss of use of and access to their financial accounts and/or credit;
- money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;
- impairment of their credit scores, ability to borrow, and/or ability to obtain credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;
- costs and lost time obtaining credit reports in order to monitor their credit records;
- anticipated future costs from the purchase of credit monitoring and/or identity theft protection services;
- costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;
- money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;
- lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach, including but not limited to efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;
- loss of the opportunity to control how their personal information is used; and

- continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Defendant Yahoo fails to undertake appropriate, legally required steps to protect the personal information in its possession.

40. The risks associated with identity theft are serious. "While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit."[21]

41. Further, criminals often trade it on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publically available.

42. To date, Yahoo has not offered Plaintiff and the Class Members any compensation from the past, present, and future harm they may experience as a result of the data breach. Yahoo has not offered any form of credit monitoring services, and has therefore failed to protect Plaintiff and the Class Members against fraud and identity theft which may occur as a result of the data breach.

43. That Yahoo failed to take appropriate measures to protect Plaintiff and the Class Members' PII is demonstrated by prior data breaches in 2012 and 2014.[22]

44. Yahoo failed to identify, implement, maintain and/or monitor appropriate data

---

[21] TRUE IDENTITY PROTECTION: IDENTITY THEFT OVERVIEW, http://www.idwatchdog.com/tikia//pdfs/Identity-Theft-Overview.pdf (visited Sept. 23, 2016).

[22] Doug Gross, *Yahoo Hacked, 450,000 Passwords Posted Online* (CNN) (July 13, 2012, 9:21 AM) http://www.cnn.com/2012/07/12/tech/web/yahoo-users-hacked/; Gary Davis, *Cybercriminals Hit T-Mobile & Yahoo! In First Week Of 2014* (MCAFEE) (Jan. 8, 2014), https://blogs.mcafee.com/consumer/cybercriminals-hit-t-mobile-yahoo-in-first-week-of-2014/ (last visited Sept. 23, 2016).

security measures, policies, procedures, controls, protocols, and software and hardware systems to ensure the security of Plaintiff and Class Members' PII.

45. Additionally, Plaintiff and Class Members' PII was improperly handled and stored, and in some cases, either unencrypted or improperly partially encrypted, inadequately protected, readily able to be copied by data thieves, and not kept in accordance with basic security protocols.[23]

46. Had Yahoo taken appropriate security measures, the Data Breach would not have occurred.

CLASS ACTION ALLEGATIONS

47. Pursuant to FED. R. CIV. P. 23, Plaintiff brings this action against Yahoo as a class action on behalf of themselves and all members of the following class of similarly situated persons (the "Class"):

> "All persons who reside in New York whose PII was compromised as a result of the Data Breach."

48. Plaintiff reserves the right to modify or amend the Class definition before the court determines whether class certification is appropriate.

49. Excluded from the Class are: (i) Defendant and any entities in which Defendant has a controlling interest; (ii) any entities in which Defendant's officers, directors, or employees are employed and any of the legal representatives, heirs, successors, or assigns of Defendant; (iii) the Judge to whom this case is assigned and any member of the Judge's immediate family and any other judicial officer assigned to this case; and (iv) all governmental entities.

[23] Bob Lord, *An Important Message About Yahoo User Security Yahoo,* YAHOO! (Sept. 22, 2016), https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security (last visited Sep. 23, 2016).

50. The members of the Class are so numerous that their joinder is impracticable. According to Yahoo, there are 500 million of Class Members. Their identities, and email addresses can be easily derived from Yahoo's internal records.

51. The rights of Plaintiff, and each Class Member, were violated in precisely the same manner by Yahoo's reckless and negligent actions, inaction, and omissions that caused the Data Breach, and the unauthorized release and disclosure of their PII.

52. There are questions of law and fact common to the Class, as a whole. The common questions of law and fact predominate over any questions affecting only individual Members of the Class, and include, without limitation:

a. Whether Yahoo had a duty to protect Plaintiff's and the Class Members' PII;

b. Whether Yahoo breached it duty to protect Plaintiff's and the Class Members' PII;

c. Whether Yahoo's breach of a legal duty caused its systems to be compromised, resulting in the loss and/or potential loss of over 500 million user accounts;

d. Whether Yahoo properly designed, adopted, implemented, controlled, managed and monitored data security processes, control, policies, procedures and/or protocols to protect Plaintiff's and the Class Members' PII in the Data Breach;

e. Whether Yahoo failed to timely inform Plaintiff and the Class Members of the Data Breach;

f. Whether Defendant's conduct was negligent; and

g. Whether Plaintiff and Class Members are entitled to damages.

53. Plaintiff's claims are typical of the claims of the Class Members because Plaintiff, like all Class Members, is a victim of Yahoo's wrongful actions, inaction, and omissions that caused the Data Breach, caused the unauthorized release and disclosure of their PII. Plaintiff and his counsel will fairly and adequately represent the interests of the Class Members. Plaintiff has no interests antagonistic to, or in conflict with, other Class Members' interests. Plaintiff's

counsel is highly experienced in the prosecution of complex commercial litigation, consumer class actions, and data breach cases.

54. A class action provides a fair and efficient method, if not the only method, for adjudicating this controversy. The substantive claims of the representative Plaintiff and the Classes are nearly identical and will require evidentiary proof of the same kind and application of the same law. There is no plain, speedy or adequate remedy other than by maintenance of this class action.

55. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because class members number in the thousands and individual joinder is impracticable. The expense and burden of individual litigation would make it impracticable or impossible for proposed class members to prosecute their claims individually. Trial of Plaintiff and the Class Members' claims is manageable. Unless the Class is certified, Defendant will remain free to continue to engage in the wrongful conduct alleged herein without consequence.

56. Certification of the Class, therefore, is appropriate under FED. R. CIV. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

57. Certification of the Class, also is appropriate under FED. R. CIV. P. 23(b)(2) because Yahoo has acted, or refused to act, on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or equitable relief with respect to the Class as a whole.

58. Certification of the Class, also is appropriate under FED. R. CIV. P. 23(b)(1) because the prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for Yahoo.

59. Yahoo's wrongful actions, inaction, and omissions are generally applicable to the Class as a whole and, therefore, Plaintiff also seeks equitable remedies for the Class.

60. Yahoo's systemic policies and practices also make injunctive relief for the Class appropriate.

61. Absent a class action, Yahoo will retain the benefits of its wrongdoing despite its serious violations of the law and infliction of economic damages, injury, and harm on Plaintiff and Class Members.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
New York General Business Law § 349

62. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

63. Plaintiff brings this claim on behalf of himself and the Class.

64. New York General Business Law § 349 ("GBL 349") makes unlawful deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in this state.

65. Defendant engaged in false and misleading marketing concerning the maintenance of Plaintiff and Class Members' PII in connection with their Yahoo user accounts.

66. In the course of Yahoo's business, trade, commerce or furnishing of any service, it willfully failed to disclose that its cybersecurity systems were inadequately protected and that its cybersecurity policies and procedures were inadequately implemented. In turn, Yahoo willfully made affirmative representations that customers' PII would be safe in its hands.

67. Furthermore, Yahoo failed to timely disclose the Breach to Plaintiff and Class Members; indeed, Yahoo has known for weeks that the data was compromised.[24]

[24] *See* Paula Blake, *Yahoo Reveals Massive Breach Of Data From 500M Accounts*, ABC NEWS (Sept. 22, 2016, 11:15 PM), http://abcnews.go.com/Technology/info-500-million-accounts-

68. Accordingly, Yahoo made untrue, deceptive, and misleading representations of material facts and omitted and/or concealed material facts to Plaintiff and the Class.

69. In reality, Yahoo failed to provide adequate protection to its customers' PII, resulting in the Breach.

70. The security of Yahoo's data systems was a material fact to Plaintiff and the Class. Had Plaintiff and the Class known of Yahoo's representations and omissions as described herein, they would not have provided their PII to Defendant.

71. Plaintiff and the Class suffered injury caused by Yahoo's affirmative statements, as well as its failure to disclose material information.

72. Plaintiff and the Class also suffered injury owing to the diminution in value of their PII.

73. Pursuant to GBL 349, Plaintiff and the Class are entitled to recover the greater of actual damages or $50. Because Yahoo acted willfully or knowingly as described herein, Plaintiff and the Class are entitled to recover three times their actual damages, up to $1,000.

SECOND CAUSE OF ACTION
Negligence

74. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

75. Plaintiff brings this claim on behalf of himself and the Class.

76. Plaintiff and Class Members were required to provide Yahoo with certain PII in connection with their Yahoo user accounts. Yahoo collected and stored this information including their names, birthdays and passwords.

---

stolen-yahoo-state-sponsored/story?id=42286309 (stating that Yahoo launched an internal investigation in July 2016 following media reports of an alleged hacker).

77. Yahoo had a duty to Plaintiff and Class Members to safeguard and protect their PII.

78. Yahoo assumed a duty of care to use reasonable means to secure and safeguard this PII, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

79. Yahoo had full knowledge about the sensitivity of Plaintiff and Class Members' PII, as well as the type of harm to could occur if such PII was wrongfully disclosed.

80. Yahoo had a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with user PII data.

81. Yahoo breached its duty of care by failing to secure and safeguard the PII of Plaintiff and Class Members. Yahoo negligently stored and/or maintained its systems.

82. Further, Yahoo , by and through its above negligent actions and/or inaction, further breached its duties to Plaintiff and Class Members by failing to design, adopt, implement, control, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Class Members' PII within its possession, custody and control.

83. Plaintiff and the other Class Members have suffered harm as a result of Defendant's negligence. These victims' loss of control over the compromised PII subjects each of them to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either use of the compromised information, or access to their user accounts.

84. It was reasonably foreseeable -- in that Defendant knew or should have known -- that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such PII, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

85. But for Defendant's negligent and wrongful breach of its responsibilities and duties owed to Plaintiff and Class Members, their PII would not have been compromised.

86. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class Members' PII, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm -- for which they are entitled to compensation. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence/negligent misrepresentation.

87. Plaintiff and Class Members are entitled to injunctive relief as well as actual and punitive damages.

THIRD CAUSE OF ACTION

Breach of Contract

88. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

89. Plaintiff brings this claim on behalf of himself and the Class.

90. Yahoo's Privacy Policy, which is incorporated in Yahoo's Terms of Service, forms a contract between Yahoo and Yahoo account holders.

91. Yahoo requires account holders to provide various types of personal information in connection with Yahoo user accounts.

92. Plaintiff and Class Members provided their PII in connection with their Yahoo user accounts.

93. Yahoo's Privacy Policy explicitly states that Yahoo's "has physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you."[25] Yahoo's also states that it will "not rent, sell or share personal information about you with other people or non-affiliated companies except to provide products or services, improve our services, contact you, conduct research, and provide anonymous reporting for

[25] *See* YAHOO!: PRIVACY POLICY, https://policies.yahoo.com/sg/en/yahoo/privacy/index.htm (last visited Sept. 23, 2016).

internal and external clients."[26]

94. Under the terms of the agreement, Yahoo's was obligated to maintain the security of Plaintiff and the Class Members' PII.

95. Plaintiff and the Class Members relied upon these terms and would not have disclosed their PII without assurances that it would be properly safeguarded.

96. Plaintiff and the Class Members fulfilled their obligations under the contract by providing their PII to Yahoo.

97. However, Yahoo failed to safeguard and protect Plaintiff's and the Class Members' PII. In permitting the Data Breach, Yahoo's breached the terms of Yahoo's Privacy Policy.

98. As the direct and proximate result of Yahoo's breaches of the contracts between Yahoo and Plaintiff and Class Members, Plaintiff and the Class Members sustained actual losses and damages as described above.

99. Accordingly, Plaintiff, on behalf of himself and the Class Members, respectfully requests this Court award all relevant damages for Yahoo's breach of contract.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment as follows:

A. For an Order certifying the proposed Class pursuant to FED. R. CIV. P. 23(b)(1), (2) and/or (3), requiring notice thereto to be paid by Yahoo and appointing Plaintiff and their counsel to represent the Class;

B. For appropriate injunctive relief and/or declaratory relief, including an order requiring Yahoo to immediately secure and fully encrypt all confidential information, to store any computer passwords in a location separate from the computers, to properly secure computers containing confidential information, to cease negligently storing, handling, and securing its

[26] *Id.*

employees' confidential information, and to provide identity theft monitoring for an additional five years;

C. Adjudging and decreeing that Yahoo has engaged in the conduct alleged herein;

D. For compensatory and general damages according to proof on certain causes of action;

E. For reimbursement, restitution and disgorgement on certain causes of action;

F. For both pre and post-judgment interest at the maximum allowable rate on any amounts awarded;

G. For costs of the proceedings herein;

H. For an Order awarding Plaintiff and the Class reasonable attorneys' fees and expenses for the costs of this suit; and

I. For any and all such other and further relief that this Court may deem just and proper, including but not limited to punitive or exemplary damages.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury of all claims and causes of action in this lawsuit to which he is so entitled.

Dated: November 18, 2016 Respectfully submitted,

By: *s/ Jeremiah Frei-Pearson*
Jeremiah Frei-Pearson
D. Greg Blankinship
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP.
445 Hamilton Ave, Suite 605
White Plains, New York 10601
Telephone: (914) 298-3281
Fax: (914) 908-6709
Jfrei-pearson@fbfglaw.com
gblankinship@fbfglaw.com

ROBINSON CALCAGNIE, INC.
Daniel S. Robinson (pro hac vice forthcoming)
Wesley K. Polischuk (pro hac vice forthcoming)
Genevieve R. Micek (pro hac vice forthcoming)
19 Corporate Plaza Drive
Newport Beach, California 92660
Telephone: (949) 720-1288
Facsimile: (949) 720-1292
drobinson@robinsonfirm.com
wpolischuk@ robinsonfirm.com

Counsel for Plaintiff and the Class